

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
24 December 2003 (24.12.2003)

PCT

(10) International Publication Number
WO 03/107588 A1

(51) International Patent Classification⁷: **H04L 9/32**
(21) International Application Number: **PCT/IB03/02337**
(22) International Filing Date: **27 May 2003 (27.05.2003)**
(25) Filing Language: **English**
(26) Publication Language: **English**
(30) Priority Data:
02077422.0 **17 June 2002 (17.06.2002)** **EP**

(71) Applicant (for all designated States except US): **KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL];**
Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **LENOIR, Petrus, J. [NL/NL];** c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **TALSTRA, Johan, C. [NL/NL];** c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **VAN DEN HEUVEL, Sebastiaan, A., F., A. [NL/NL];** c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **STARING, Antonius, A., M. [NL/NL];** c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **GROENENDAAL, Antonius, W., M.;** Philips Intellectual Property & Standards, Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States (national): **AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.**

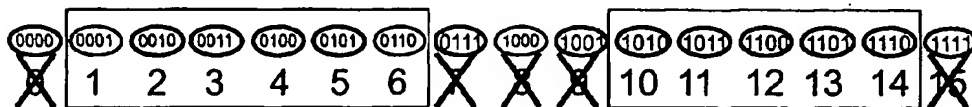
(84) Designated States (regional): **ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),** Eurasian patent (**AM, AZ, BY, KG, KZ, MD, RU, TJ, TM**), European patent (**AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR**), OAPI patent (**BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG**).

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: **SYSTEM FOR AUTHENTICATION BETWEEN DEVICES USING GROUP CERTIFICATES**



$S_{0,7}$

$S_{9,15}$

(57) Abstract: In whitelist-based authentication, a first device (102) in a system (100) authenticates itself to a second device (103) using a group certificate identifying a range of non-revoked device identifiers, said range encompassing the device identifier of the first device (102). Preferably the device identifiers correspond to leaf nodes in a hierarchically ordered tree, and the group certificate identifies a node (202-207) in the tree representing a subtree in which the leaf nodes correspond to said range. The group certificate can also identify a further node (308, 310, 312) in the subtree which represents a sub-subtree in which the leaf nodes correspond to revoked device identifiers. Alternatively, the device identifiers are selected from a sequentially ordered range, and the group certificate identifies a subrange of the sequentially ordered range, said subrange encompassing the whitelisted device identifiers.

WO 03/107588 A1